



## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

[Docket No. 230814-0193]

#### Request for Comments on draft FIPS-203, draft FIPS-204, and draft FIPS-205

**AGENCY:** National Institute of Standards and Technology (NIST), Commerce.

**ACTION:** Notice; request for comments.

**SUMMARY:** The National Institute of Standards and Technology (NIST) requests comments on three draft Federal Information Processing Standards (FIPS): FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-based Digital Signature Standard. These proposed standards specify key establishment and digital signature schemes that are designed to resist future attacks by quantum computers, which threaten the security of current standards. The three algorithms specified in these standards are each derived from different submissions in the NIST post-quantum cryptography standardization project (see: <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization>).

**DATES:** Comments on FIPS 203, FIPS 204, or FIPS 205 must be received on or before

[INSERT DATE 90 DAYS AFTER PUBLICATION OF THIS NOTICE IN THE  
FEDERAL REGISTER].

**ADDRESSES:** The drafts of FIPS 203, FIPS 204, and FIPS 205 are available for review and comment on the NIST Computer Security Resource Center website at <https://csrc.nist.gov> and at [www.regulations.gov](https://www.regulations.gov). Comments on FIPS 203 may be sent electronically to [FIPS-203-comments@nist.gov](mailto:FIPS-203-comments@nist.gov) with “Comment on FIPS 203” in the subject line or submitted via [www.regulations.gov](https://www.regulations.gov). Comments on FIPS 204 may be sent electronically to [FIPS-204-comments@nist.gov](mailto:FIPS-204-comments@nist.gov) with “Comment on FIPS 204” in the

subject line or via [www.regulations.gov](http://www.regulations.gov). Comments on FIPS 205 may be sent electronically to [FIPS-205-comments@nist.gov](mailto:FIPS-205-comments@nist.gov) with “Comment on FIPS 205” in the subject line or via [www.regulations.gov](http://www.regulations.gov). Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: FIPS Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930.

All relevant comments received by the deadline will be published electronically at <https://csrc.nist.gov> and [www.regulations.gov](http://www.regulations.gov) without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be posted or considered.

After the comment period closes, NIST will analyze the comments, make changes to the documents as appropriate, and then propose the drafts FIPS 203, FIPS 204, and FIPS 205 to the Secretary of Commerce for approval.

**FOR FURTHER INFORMATION CONTACT:** Dr. Dustin Moody,

National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: [Dustin.Moody@nist.gov](mailto:Dustin.Moody@nist.gov), phone: (301) 975–8136.

**SUPPLEMENTARY INFORMATION:** Over the past several years, there has been steady progress toward building quantum computers. The security of many commonly used public-key cryptosystems would be at risk if large-scale quantum computers were ever realized. In particular, this would include key-establishment schemes and digital signatures that are based on integer factorization and discrete logarithms (both over finite fields and elliptic curves). As a result, in 2017, the National Institute of Standards and Technology (NIST) initiated a public process to select quantum-resistant public-key cryptographic algorithms for standardization. These quantum-resistant algorithms would augment the public-key cryptographic algorithms already contained in FIPS 186-5,

Digital Signature Standard (DSS), as well as NIST Special Publication (SP) 800-56A Revision 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, and SP 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography.

NIST issued a public call for submissions to the Post-Quantum Cryptography (PQC) Standardization Process in December 2016. Prior to the November 2017 deadline, a total of 82 candidate algorithms were submitted. Shortly thereafter, the 69 candidates that met both the submission requirements and the minimum acceptability criteria were accepted into the first round of the standardization process. Submission packages for the first-round candidates were posted online for public review and comment.

After a year-long review of the candidates, NIST selected 26 algorithms to move on to the second round of evaluation in January 2019. These algorithms were viewed as the most promising candidates for eventual standardization, and were selected based on both internal analysis and public feedback. During the second round, there was continued evaluation by NIST and the broader cryptographic community. After consideration of these analyses and other public input received throughout the evaluation process, NIST selected seven finalists and eight alternates to move on to the third round in July 2020.

The third round began in July 2020 and continued for approximately 18 months. During the third round, there was a more thorough analysis of the theoretical and empirical evidence used to justify the security of the candidates. There was also careful benchmarking of their performance using optimized implementations on a variety of software and hardware platforms. Similar to the first two rounds, NIST also held the (virtual) Third NIST PQC Standardization Conference in June 2021. NIST summarized its decisions in a report at the end of each round; NISTIR 8240 for the first round, NISTIR 8309 for the second round, and NISTIR 8413 for the third round. These reports

are available at <https://csrc.nist.gov/publications/ir>.

After three rounds of evaluation and analysis, NIST selected four algorithms it will standardize as a result of the PQC Standardization Process. The public-key encapsulation mechanism selected was CRYSTALS–KYBER, along with three digital signature schemes: CRYSTALS–Dilithium, FALCON, and SPHINCS+. It is intended that these algorithms will be capable of protecting sensitive U.S. Government information well into the foreseeable future, including after the advent of quantum computers.

The draft of FIPS 203 specifies a cryptographic scheme called Module Learning with errors Key Encapsulation Mechanism, or MLWE-KEM, which is derived from the CRYSTALS-KYBER submission. A Key Encapsulation Mechanism (or KEM) is a particular type of key establishment scheme which can be used to establish a shared secret key between two parties communicating over a public channel. Current NIST-approved key establishment schemes are specified in SP 800-56A *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm-Based Cryptography* and SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*.

The drafts of FIPS 204 and 205 each specify digital signature schemes, which are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. FIPS 204 specifies the Module Learning with errors Digital Signature Algorithm, or ML-DSA, which is derived from CRYSTALS-Dilithium submission. FIPS 205 specifies the Stateless Hash-based Digital Signature Algorithm, or SLH-DSA, derived from the SPHINCS+ submission. Current NIST-approved digital signature schemes are specified in FIPS 186-5, *Digital Signature Standard* and SP 800-208, *Recommendation for Stateful Hash-based Signature Schemes*. In the future, NIST intends to develop a FIPS specifying

a digital signature algorithm derived from FALCON as an additional alternative to these standards.

Authority: 40 U.S.C. 11331(f), 15 U.S.C. 278g-3.

**Alicia Chambers,**

*NIST Executive Secretariat.*

[FR Doc. 2023-18197 Filed: 8/23/2023 8:45 am; Publication Date: 8/24/2023]